DIFFERENCE METHODS AND FERRERO PAIRS

TIM BOYKETT AND PETER MAYR

Institut für Algebra, Stochastik und
wissensbasierte mathematische Systeme,
Johannes Kepler Universität Linz,
4040 Linz, Austria
`tim@algebra.uni-linz.ac.at`
`peter.mayr@algebra.uni-linz.ac.at`

ABSTRACT. We present a construction method of BIB-designs from a finite group G and a group of automorphisms Φ on G such that $|\Phi(x)| = |\Phi|$ for all $x \in G$, $x \neq 0$. By using a generalization of the concept of a difference family we can so unify several previous constructions of BIB-designs from planar near-rings.

1. INTRODUCTION

This paper introduces a general construction that encompasses several known constructions of designs from near-rings. The original work of Ferrero, lying historically between that of Bose and Wilson, introduced the construction, related to difference families. This paper uses a slightly more general concept, the short difference family, to generalize these constructions.

We proceed first by introducing our terminology, then the short difference family construct. We show that such constructions arise naturally from fixed-point-free automorphism groups acting on groups.

2. DESIGNS AND DIFFERENCE FAMILIES

Let V be a set of size v with $v > 1$. Let k, λ be positive integers. For our purposes, a (v, k, λ)-*BIB-design* (or *design* for short) is a set $\mathbf{B}$ of subsets of V that satisfies the following conditions:

(1) $|B| = k$ for all $B \in \mathbf{B}$;
(2) $|\{B \in \mathbf{B} \mid u, v \in B\}| = \lambda$ for all $u, v \in V, u \neq v$.

The elements of V are usually referred to as points; the elements of $\mathbf{B}$ are called blocks. By our definition a design does not have repeated (multiple) blocks. Apart from that our definition is equivalent to that of a 2-balanced design [BJL99, p. 15] or (v, k, λ)-BIBD [CD96].

An *automorphism* of a design $\mathbf{B}$ is a bijection of V that fixes $\mathbf{B}$.

In this note we will use the following concepts: Let $(G, +)$ be a finite group, not necessarily abelian, of order $v > 1$. We denote $G \setminus \{0\}$ by G^*. The group G acts on itself by right translation. For $B \subseteq G$, we let $G_B = \{g \in G \mid B + g = B\}$ denote the stabilizer of the set B under the action of G.

Let $\mathbf{B}$ be a set of subsets of G. Then $\mathrm{dev}\mathbf{B} = \{B + g \mid B \in \mathbf{B}, g \in G\}$ is called the *development* of $\mathbf{B}$ in G. For $B, C \in \mathbf{B}$, we define

$$B \sim C \text{ if and only if } \exists g \in G : B = C + g.$$

This relation $\sim$ is an equivalence relation on $\mathbf{B}$. The equivalence class of $B \in \mathbf{B}$ modulo $\sim$ is denoted by $B/\sim$.

Definition 2.1. Let $\mathbf{B}$ be a set of subsets of the group $(G, +)$ with $|G| > 1$. Let $v = |G|$, and let k, μ, ν, λ' be positive integers such that the following are satisfied:

(1) $|B| = k$ for all $B \in \mathbf{B}$;
(2) $|G_B| = \mu$ for all $B \in \mathbf{B}$;
(3) $|B/\sim| = \nu$ for all $B \in \mathbf{B}$;
(4) $|\{(B, a, b) \mid B \in \mathbf{B}, a, b \in B, a - b = d\}| = \lambda'$ for all $d \in G, d \neq 0$.

Then $\mathbf{B}$ is called a $(v, k, \frac{\lambda'}{\mu\nu})$-*short difference family* (or *sdf*) in G.

We note that an sdf with $\mu = 1$ is in fact a (v, k, λ)-difference family as defined in [BJL99, p. 470]. However, the general definition of a difference family allows multiple blocks, which we avoid. The term short difference family seems appropriate since in the literature a block $B \in \mathbf{B}$ with $|G_B| > 1$ is said to have a short orbit.

In [CD96, p.271] a set of subsets $\mathbf{B}$ of G is called a partial difference family if $\mathrm{dev}\mathbf{B}$ is a BIB-design. The following proposition says that short difference families are partial difference families in this sense.

Proposition 2.2. *Let $\mathbf{B}$ be a (v, k, λ)-sdf in the group G. Then $\mathrm{dev}\mathbf{B}$ is a (v, k, λ)-design.*

We note that G acts as group of design-automorphisms on $\mathrm{dev}\mathbf{B}$ for an sdf $\mathbf{B}$. Hence the automorphism group of $\mathrm{dev}\mathbf{B}$ acts transitively on the point set G of $\mathrm{dev}\mathbf{B}$.

Proof of Proposition 2.2. Let $\mathbf{B}$ be a (v, k, λ)-sdf. Then there exist μ, ν such that $|G_B| = \mu$ and $|B/\sim| = \nu$ for all $B \in \mathbf{B}$. We have $|\{(B, a, b) \mid B \in \mathbf{B}, a, b \in B, a - b = d\}| = \lambda\mu\nu$ for all $d \in G, d \neq 0$.

If $B \sim C$ for $B, C \in \mathbf{B}$, then $\mathrm{dev}\{B\} = \mathrm{dev}\{C\}$. Let $\mathbf{R}$ be a set of representatives of $\sim$ on $\mathbf{B}$. Then

$$\mathrm{dev}\mathbf{B} = \bigcup_{B \in \mathbf{R}} \mathrm{dev}\{B\},$$

where the union is disjoint.

Let $u, v \in G, u \neq v$. We count the number of blocks in $\mathrm{dev}\mathbf{B}$ that contain $\{u, v\}$:

$$
\begin{aligned}
|\{C \in \mathrm{dev}\mathbf{B} \mid u, v \in C\}| &= \sum_{B \in \mathbf{R}} |\{C \in \mathrm{dev}\{B\} \mid u, v \in C\}| \\
&= \sum_{B \in \mathbf{B}} \frac{|\{C \in \mathrm{dev}\{B\} \mid u, v \in C\}|}{|B/\sim|} \\
&= \frac{1}{\nu} \sum_{B \in \mathbf{B}} \frac{|\{g \in G \mid u, v \in B + g\}|}{|G_B|} \\
&= \frac{1}{\mu\nu} \sum_{B \in \mathbf{B}} |\{g \in G \mid u - g, v - g \in B\}|
\end{aligned}
$$

For $B \in \mathbf{B}$ fixed, we now consider the map $f : \{g \in G \mid u - g, v - g \in B\} \to \{(a, b) \in B \times B \mid a - b = u - v\}, g \mapsto (u - g, v - g)$. Then f has an inverse, given by $f^{-1} : (a, b) \mapsto -a + u$. In particular, f is bijective. Hence we obtain

$$
\begin{aligned}
|\{C \in \mathrm{dev}\mathbf{B} \mid u, v \in C\}| &= \frac{1}{\mu\nu} \sum_{B \in \mathbf{B}} |\{(a, b) \in B \times B \mid a - b = u - v\}| \\
&= \frac{1}{\mu\nu} \cdot |\{(B, a, b) \mid B \in \mathbf{B}, a, b \in B, a - b = u - v\}| \\
&= \frac{1}{\mu\nu} \cdot \lambda\mu\nu \\
&= \lambda.
\end{aligned}
$$

Thus each set $\{u, v\}$ with $u, v \in G, u \neq v$, is contained in λ distinct blocks of $\mathrm{dev}\mathbf{B}$. This completes the proof that $\mathrm{dev}\mathbf{B}$ is a (v, k, λ)-design. $\square$

In the proof above we used that a set of representatives $\mathbf{R}$ for $\sim$ on $\mathbf{B}$ has the same development as $\mathbf{B}$. Now each equivalence class of $\sim$ on R has size 1. Thus we could have required $|B/\sim| = 1$ for all $B \in \mathbf{B}$ instead of condition (3) in our definition of an sdf, and we would still obtain the same designs. It is just a matter of notational convenience that we allow $|B/\sim| = \nu$ for an arbitrary, but fixed integer ν.

In the following lemma G_B is characterized as the unique maximal subgroup of which $B \subseteq G$ can be expressed as union of left cosets.

Lemma 2.3. *Let G be a group, and let $B \subseteq G$. Then G_B is the unique maximal (with respect to containment) element in $\{H \leq G \mid B = B + H\}$.*

Proof. Straightforward. ☐

As a corollary of Lemma 2.3, we obtain that $G_B = \{0\}$ if $|B|$ and $|G|$ are relatively prime.

3. SHORT DIFFERENCE FAMILIES FROM FPF AUTOMORPHISMS

Let $(G, +)$ be a finite group. We denote the identity mapping on G by $\mathbf{1}$, and let $\mathbf{0} : G \to G, x \mapsto 0$. A group Φ of automorphisms on $(G, +)$ is said to be *fixed-point-free (fpf)* iff $|\Phi(x)| = |\Phi|$ for all $x \in G^*$.

Proposition 3.1. *Let Φ be group of fpf automorphisms on $(G, +)$, and let $S \subseteq \Phi \cup \{\mathbf{0}\}$ with $|S| > 1$. Let μ, ν be positive integers such that the following are satisfied:*

(1) $|G_{S(a)}| = \mu$ *for all $a \in G^*$;*
(2) $|S(a)/\sim| = \nu$ *for all $a \in G^*$.*

Then $\{S(x) \mid x \in G^*\}$ is a $(|G|, |S|, \frac{|S| \cdot (|S|-1)}{\mu\nu})$-sdf.

Proof. Since Φ is fpf, we have $|S(x)| = |S|$ for all $x \in G^*$. We note that for the same reason the map $\alpha - \beta : G \to G, x \mapsto \alpha(x) - \beta(x)$ is bijective for all $\alpha, \beta \in \Phi \cup \{\mathbf{0}\}, \alpha \neq \beta$. Thus $(\alpha - \beta)^{-1}$ exists.

It remains to check condition (4) of Definition 2.1. Let $d \in G^*$, and let $\mathbf{B} = \{S(x) \mid x \in G^*\}$. Now we have

$$
\begin{aligned}
\{(B, a, b) \mid B \in \mathbf{B}, a, b \in B, a - b = d\} &= \\
= \quad \{(S(x), \alpha(x), \beta(x)) \mid x \in G^*, \alpha, \beta \in S, \alpha(x) - \beta(x) = d\} &= \\
= \quad \{(S(x), \alpha(x), \beta(x)) \mid \alpha, \beta \in S, \alpha \neq \beta, x = (\alpha - \beta)^{-1}(d)\},
\end{aligned}
$$

and the cardinality of the last set is $|S| \cdot (|S| - 1)$. Thus $\mathbf{B}$ is an sdf with parameters as given in the proposition. ☐

Several of the designs from planar near-rings as described in [Cla92] arise in the situation of Proposition 3.1 for different choices of a set S of endomorphisms on a group G. We will not prove the next 2 well-known results. We note that also for the original proofs the difficulty lies entirely in verifying the conditions (1) and (2) as given in Proposition 3.1.

Corollary 3.2. [Cla92, cf. p. 59, Theorem 5.5] *Let Φ be fpf on G. Then* $\mathrm{dev}\{\Phi(x) \mid x \in G^*\}$ *is a $(|G|, |\Phi|, |\Phi| - 1)$-design.*

Corollary 3.3. *Let Φ be fpf on G. Let $S = \Phi \cup \{0\}$, and let $\mathbf{B} = \{S(x) \mid x \in G^*\}$.*

(1) [Cla92, cf. p. 118, Theorem 7.9] *If B is not a subgroup of G for any $B \in \mathbf{B}$, then $\mathrm{dev}\mathbf{B}$ is a $(|G|, |\Phi| + 1, |\Phi| + 1)$-design.*
(2) [Cla92, cf. p. 118, Theorem 7.11] *If B is a subgroup of G for all $B \in \mathbf{B}$, then $\mathrm{dev}\mathbf{B}$ is a $(|G|, |\Phi| + 1, 1)$-design.*

Proposition 3.4. *Let Φ be fpf on G, and let $S \subseteq \Phi \cup \{0\}$. Let Ψ be a group of automorphisms of G, such that Ψ normalizes S and Ψ is transitive on G^*.*

Then $\mathbf{B} = \{S(x) \mid x \in G^*\}$ is an sdf, and $G \rtimes \Psi$ acts as a doubly transitive group of automorphisms on $\mathrm{dev}\mathbf{B}$.

Proof. It suffices to check that the assumptions of Proposition 3.1 are satisfied. Let $a, b \in G^*, c \in G$ such that $S(a) = S(b) + c$, and let $\psi \in \Psi$. Since ψ normalizes S, we have $S(\psi(a)) = S(\psi(b)) + \psi(c)$. Thus we obtain $|G_{S(\psi(a))}| = |G_{S(a)}|$ and $|S(\psi(a))/ \sim | = |S(a)/ \sim |$. Since Ψ is transitive on G^*, the assumptions of Proposition 3.1 are satisfied. The result follows. $\square$

Corollary 3.5. *Let $(F, +, \cdot)$ be a finite left near-field, and let $S \subseteq F$ such that $xS = Sx$ for all $x \in F$. Then $\mathbf{B} = \{Sx \mid x \in F^*\}$ is an sdf.*

Proof. Straightforward by Proposition 3.4. $\square$

We note that the assumption $xS = Sx$ for all $x \in F$ in the above corollary is trivially fulfilled if $(F, +, \cdot)$ is a field.

4. A GENERALIZATION OF SUN'S SEGMENTS

We will now describe how the designs of segments as defined in [Sun01] fit into our setting of short difference families. Our main result is the following.

Proposition 4.1. *Let $(G, +)$ be a group, and let S be a set of endomorphisms on G such that the following conditions are satisfied:*

(1) $\mathbf{0}, \mathbf{1} \in S$ *and* $|S| > 2$;
(2) $\{\mathbf{1} - \alpha \mid \alpha \in S\} = S$;
(3) $\langle S^* \rangle$ *is a group of fpf automorphisms on G.*

We assume that $|G|$ and $|\langle S^* \rangle|$ are odd. Then $\{S(x) \mid x \in G^*\}$ is a $(|G|, |S|, \frac{|S| \cdot (|S|-1)}{2})$-sdf.

Throughout this section we assume that $(G, +)$ is a group with a set of endomorphisms S that satisfy the conditions (1), (2), and (3) of Proposition 4.1.

As an example of such a set S, we may consider a group of fpf automorphisms Φ on G such that 6 divides $|\Phi|$. Now let $S = \{\alpha \in \Phi \mid \mathrm{ord}\alpha = 6\} \cup \{\mathbf{0}, \mathbf{1}\}$. We show that if $\alpha \in \Phi$ has order 6, then $\alpha^5 = \mathbf{1} - \alpha \in \Phi$.

Let $\alpha \in \Phi$ with $\mathrm{ord}\alpha = 6$. Then α^3 is an fpf automorphism of order 2. Thus $\alpha^3 = -\mathbf{1}$ is an automorphism of G, and hence G is abelian. Let $x \in G$. By $\alpha^2(x + \alpha^2(x) + \alpha^4(x)) = \alpha^2(x) + \alpha^4(x) + x$ we find that $x + \alpha^2(x) + \alpha^4(x)$ is a fixed-point of $\alpha^2 \neq \mathbf{1}$. Thus $x + \alpha^2(x) + \alpha^4(x) = 0$ for all $x \in G$. Now $\mathbf{1} + \alpha^2 + \alpha^4 = \mathbf{0}$ yields $\mathbf{1} + \alpha^4 = -\alpha^2$. By $\alpha^3 = -\mathbf{1}$, we obtain $\mathbf{1} - \alpha = \alpha^5$.

For the proof of Proposition 4.1, we need a bit of preparation.

Lemma 4.2. *Let α be an automorphism on $(G, +)$ such that $\mathbf{1} - \alpha$ is also an automorphism on $(G, +)$. Then $(G, +)$ is abelian.*

Proof. Let $\beta = \mathbf{1} - \alpha$, and let $x, y \in G$. Then we have

$$(4.1) \qquad \beta(x + y) = x + y - \alpha(x + y) = x + y - \alpha(y) - \alpha(x)$$

and

$$(4.2) \qquad \beta(x + y) = \beta(x) + \beta(y) = x - \alpha(x) + y - \alpha(y).$$

By (4.1) and (4.2), we obtain

$$(4.3) \qquad (y - \alpha(y)) - \alpha(x) = -\alpha(x) + (y - \alpha(y)).$$

Since $-\alpha$ and $\mathbf{1} - \alpha$ are bijections on G, equation (4.3) yields $a + b = b + a$ for all $a, b \in G$. $\qquad\square$

Lemma 4.3. *Let Φ be fpf on $(G, +)$, and let $\varphi \in \Phi$. If $\{\alpha, \mathbf{1} - \alpha\} \subseteq N_\Phi(\langle \varphi \rangle)$, then $\{\alpha, \mathbf{1} - \alpha\} \subseteq C_\Phi(\langle \varphi \rangle)$.*

Proof. Let $\{\alpha, \mathbf{1} - \alpha\} \subseteq N_\Phi(\langle \varphi \rangle)$. We note that $\langle \alpha, \mathbf{1} - \alpha \rangle$ is an abelian, and hence cyclic group of fpf automorphisms. Let $\beta \in \Phi$ generate $\langle \alpha, \mathbf{1} - \alpha \rangle$, and let $\alpha = \beta^i, \mathbf{1} - \alpha = \beta^j$.

Since β normalizes $\langle \varphi \rangle$, there exists an integer r such that $\varphi^\beta = \varphi^r$. Then $\varphi^\alpha = \varphi^{(r^i)}$, and $\varphi^{1-\alpha} = \varphi^{(r^j)}$.

By $\varphi(\mathbf{1} - \alpha) = \varphi - \varphi\alpha = \varphi - \alpha\varphi^{(r^i)}$, we have $(\mathbf{1} - \alpha)\varphi^{(r^j)} = \varphi - \alpha\varphi^{(r^i)}$. Thus we obtain

$$(4.4) \qquad\qquad \alpha(\varphi^{(r^i)} - \varphi^{(r^j)}) \;=\; \varphi - \varphi^{(r^j)}.$$

If $\varphi^{(r^i)} \neq \varphi^{(r^j)}$, then $\varphi^{(r^i)} - \varphi^{(r^j)}$ is invertible because Φ is fpf. Then $\alpha = (\varphi - \varphi^{(r^j)})(\varphi^{(r^i)} - \varphi^{(r^j)})^{-1}$, and, in particular, α commutes with φ. But then also $\mathbf{1} - \alpha$ commutes with φ. We obtain $\varphi^{(r^i)} = \varphi = \varphi^{(r^j)}$ in contradiction to our assumption. Thus we have $\varphi^{(r^i)} = \varphi^{(r^j)}$, and by (4.4) $\varphi = \varphi^{(r^j)}$. Both α and $\mathbf{1} - \alpha$ commute with φ. $\qquad\square$

Corollary 4.4. *If $\langle S^* \rangle$ is metacyclic, then $\langle S^* \rangle$ is cyclic.*

Proof. Let $\Phi = \langle S^* \rangle$ be a metacyclic group of fpf automorphisms. Then there exists $\varphi \in \Phi$ such that $N = \langle \varphi \rangle$ is normal in Φ, and there exists $\psi \in \Phi$ such that ψN generates Φ/N.

By Lemma 4.3, a cyclic normal subgroup of Φ is central in Φ. In particular, ψ and φ commute. Thus Φ is abelian and hence cyclic. $\qquad\square$

We note that, by Corollary 4.4, $\Phi = \langle S^* \rangle$ is cyclic if $|\Phi|$ is odd.

Corollary 4.5. *Let S be a set of endomorphisms of $(G, +)$ such that $S = \mathbf{1} - S$ and $\Phi = \langle S^* \rangle$ is a group of fpf automorphisms of G.*
Then $\Phi/Z(\Phi)$ is trivial or isomorphic to one of the following: A_4, S_4, A_5, S_5.

Proof. By [Bro01, Theorem 1.4], we have a unique normal subgroup N of Φ such that all Sylow subgroups of N are cyclic and Φ/N is isomorphic to one of the following groups: $1, V_4, A_4, S_4, A_5, S_5$ where 1 denotes the trivial group and V_4 denotes the Klein group. We note that N' is cyclic and a normal subgroup of Φ. Thus the elements of S^* normalize N' and, by Lemma 4.3, S^* centralizes N'. Hence we have $N' \subseteq Z(\Phi)$. In particular, N is nilpotent. Now N is the direct product of its cyclic Sylow subgroups, and N is cyclic. As a cyclic normal subgroup, N is central in Φ by Lemma 4.3. Thus $N \subseteq Z(\Phi)$.

First we assume that Φ/N is abelian. Since N is central, this yields that Φ is nilpotent. Let P denote the Sylow 2-subgroup of Φ. Then P is a cyclic group or a generalized quaternion group. In any case, P has a normal cyclic subgroup R of index 2. Since Φ is the direct product of its Sylow subgroups, R is normal in Φ. By Lemma 4.3, R is central in Φ, which implies that P is cyclic. Thus Φ/N is not isomorphic to V_4.

It remains that Φ/N is isomorphic to $1, A_4, S_4, A_5$, or S_5. Since all these groups have trivial center, we finally obtain $N = Z(\Phi)$. The corollary is proved. $\square$

Lemma 4.6. *Let $a, b \in G^*, c \in G$. If $S(a) = S(b) + c$, then $-a + b + 2c \in G_{S(a)}$.*

Proof. Let $S(a) = S(b) + c$. Since $(G, +)$ is abelian and $S(x) = x - S(x)$ for all $x \in G^*$, we obtain:

$$
\begin{aligned}
S(a) - a + b + 2c &= -S(a) + b + 2c \\
&= -(S(b) + c) + b + 2c \\
&= -S(b) + b + c \\
&= S(b) + c \\
&= S(a)
\end{aligned}
$$

Thus $-a + b + 2c \in G_{S(a)}$. $\square$

Lemma 4.7. *Let $\Phi = \langle S \setminus \{0\} \rangle$. We assume that $|\Phi|$ is odd and that $G_{S(a)} = \{0\}$ for all $a \in G^*$. Then $S(a) = S(b) + c$ iff ($b = a$ and $c = 0$) or ($b = -a$ and $c = a$).*

Proof. Let $S(a) = S(b) + c$. By Lemma 4.6, we have $-a + b + 2c \in G_{S(a)}$. Since $G_{S(a)} = \{0\}$ by assumption, we obtain $b = a - 2c$ and $S(a) = S(a - 2c) + c$.

We note that $S(a - 2c)$ contains the elements 0 and $a - 2c$. By $S(a) = S(a - 2c) + c$, we obtain that $0 + c$ and $(a - 2c) + c$ are in $S(a)$. With $\{0, a\} \subseteq S(a)$ and $S(a) - c = S(a - 2c)$ we find $\{-c, a - c\} \subseteq S(a - 2c)$. Summing up, we have $\{0, a, c, a - c\} \subseteq S(a)$ and $\{0, a - 2c, -c, a - c\} \subseteq S(a - 2c)$.

Seeking a contradiction, we suppose that $c \neq a$ and $c \neq 0$. Let $S^* = S \setminus \{0\}$. Since $a - c \in S^*(a)$ and $a - c \in S^*(a - 2c)$, both $S^*(a)$ and $S^*(a - 2c)$ are contained in $\Phi(a - c)$. In particular, c and $-c$ are in $\Phi(a - c)$.

If $c = -c$, then $2c = 0$ and $S(a) = S(a) + c$. Now $G_{S(a)} = 0$ yields $c = 0$, which contradicts our assumption that $c \neq 0$.

If $c \neq -c$, then there exists $\varphi \in \Phi, \varphi \neq \mathbf{1}$, such that $\varphi(c) = -c$. Now, $c \neq 0$ is a fixed-point of φ^2. Hence $\varphi^2 = \mathbf{1}$ and $|\Phi|$ is even, which contradicts the assumption of the lemma. Thus we have $c = a$ or $c = 0$. The lemma is proved. $\square$

Proof of Proposition 4.1. Let G and S satisfy the assumptions, and let $a \in G^*$. We will prove that

$$(4.5) \qquad\qquad\qquad |G_{S(a)}| = 1.$$

Seeking a contradiction, we suppose that there exists $d \in G_{S(a)}$ such that $d \neq 0$. Since $\mathbf{0} \in S$, we then have $\{d, -d\} \in S(a)$. For $\Phi = \langle S^* \rangle$, we obtain $\{d, -d\} \in \Phi(a)$. In particular, there is $\varphi \in \Phi$ such that $\varphi(d) = -d$. We have $d \neq -d$ and $\varphi \neq \mathbf{1}$ by the assumption that $|G|$ is odd. Since φ^2 fixes $d \neq 0$, we then have $\mathrm{ord}\varphi = 2$. This contradicts the assumption that $|\Phi|$ is odd. Thus we have $d = 0$, and (4.5) is proved. Next we show that

$$(4.6) \qquad\qquad\qquad |S(a)/\sim| = 2.$$

For $b \in G^*, c \in G$ such that $S(a) = S(b) + c$, Lemma 4.7 yields that $b = a$ or $b = -a$. Thus we obtain $S(a)/\sim = \{S(a), S(-a)\}$. Since $a \neq -a$ by the assumption that $|G|$ is odd, we have $S(a) \neq S(-a)$. This proves (4.6).

Now we obtain the result from (4.5) and (4.6) with Proposition 3.1. $\square$

We give several examples for designs of segments from short difference families.

Example 4.8. If G is an elementary abelian 2-group, then we have $S = 1 - S = 1 + S$. Thus we know that $\{0, a\} \subseteq G_{S(a)}$ for all $a \in G^*$. Assume equality, that is, $G_{S(a)} = \{0, a\}$ for all $a \in G^*$. Then Lemma 4.6 yields $|S(a)/\sim| = 1$ for all $a \in G^*$. By Proposition 3.1, $\{S(a) \mid a \in G^*\}$ forms a $(|G|, |S|, \frac{|S| \cdot (|S|-1)}{2})$-sdf for G.

Example 4.9. Let $|S| = 3$, that is, $S = \{\mathbf{0}, \mathbf{1}, \mathbf{2}^{-1}\}$ where $\mathbf{2}^{-1}$ is the inverse mapping of $\mathbf{2}: G \to G, x \mapsto x + x$. Suppose there is $a \in G^*$ such that $G_{S(a)} \neq \{0\}$. Then $G_{S(a)} = S(a)$, which yields $\mathbf{2}^{-1}(a) = -a$. Hence $\mathbf{2}^{-1}$ is an fpf automorphism of order 2, and $\mathbf{2}^{-1} = \mathbf{2} = -\mathbf{1}$. Now $2x = -x$ for all $x \in G^*$ yields $3x = 0$; G is an elementary abelian 3-group. Thus $S(x) = \langle x \rangle = G_{S(x)}$ for all $x \in G$. By Proposition 3.1, $\{S(a) \mid a \in G^*\}$ forms a $(|G|, 3, 1)$-sdf for G.

If $|S| = 3$ and $G_S(a) = \{0\}$ for all $a \in G^*$, then $S(a)/\sim = \{S(a), -S(a)\}$ for all $a \in G^*$ by Lemma 4.6, and $\{S(a) \mid a \in G^*\}$ forms a $(|G|, 3, 3)$-sdf for G by Proposition 3.1.

Example 4.10. Let $S \subseteq \{\alpha \in \Phi \mid \mathrm{ord}\alpha = 6\} \cup \{\mathbf{0}, \mathbf{1}\}$ such that $\{\mathbf{0}, \mathbf{1}\} \in S$ and $\alpha^5 \in S$ for all $\alpha \in S$. Then $|S|$ is even, $|S| \leq 22$, and $\{S(a) \mid a \in G^*\}$ is a $(|G|, |S|, \frac{|S| \cdot (|S|-1)}{2})$-sdf for G.

From Corollary 4.5 we obtain that $\langle S^* \rangle$ is cyclic, isomorphic to $\mathrm{SL}(2,3)$ or to $\mathrm{SL}(2,5)$. Thus G has at most 20 fixed-point-free automorphisms of order 6, and $|S| \leq 22$.

Next we show that $G_{S(a)} = \{0\}$ for all $a \in G^*$. Let $a \in G^*$, $c \in G_{S(a)}$. Then we have $\alpha \in S$ such that $c = \alpha(a)$. Since $-c \in G_{S(a)}$, we also have $\beta \in S$ such that $-c = \beta(a)$. We note that $|G|$ is odd because $\langle S^* \rangle$ is even. Suppose that $\alpha \neq \mathbf{0}$. Then $c \neq 0$ and $\beta\alpha^{-1}(c) = -c \neq c$. By assumption $\beta\alpha^{-1}$ is fixed-point-free and has order 2. Hence $\beta\alpha^{-1} = -\mathbf{1}$ and $\beta = -\alpha$. If $\alpha = \mathbf{1}$, then we obtain $\beta = -\mathbf{1} \in S$ which contradicts the assumption on S. If $\mathrm{ord}\alpha = 6$, then $\beta = \alpha^4 \in S$ and $\mathrm{ord}\beta = 3$ which yields a contradiction. Thus we have $\alpha = 0$ and $G_{S(a)} = \{0\}$.

Next we show that $S(a)/\sim = \{S(a), -S(a)\}$ for all $a \in G^*$. Let $a, b \in G^*, c \in G$ such that $S(a) = S(b) + c$. Seeking a contradiction we suppose that $c \notin \{0, a\}$. Then we have $\alpha \in S \setminus \{\mathbf{0}, \mathbf{1}\}$ and $\beta \in S^*$ such that $c = \alpha(a)$ and $c = -\beta(b)$. We note that $\beta \neq \mathbf{1}$ because otherwise $S(a) = S(-c) + c = S(c)$ and Lemma 4.6 yields $a = c$. Hence both α and β have order 6. From Lemma 4.6 we obtain $-\alpha^{-1}(c) - \beta^{-1}(c) + 2c = 0$. Together with $\alpha^{-1} = \mathbf{1} - \alpha$ and $\beta^{-1} = \mathbf{1} - \beta$ (see the remark below Proposition 4.1), this yields $\alpha(c) + \beta(c) = 0$. Thus $\beta = \alpha^4$ by the assumption that $\langle S^* \rangle$ is fpf. This contradicts that α, β have order 6. Hence $\alpha, \beta \in \{\mathbf{0}, \mathbf{1}\}$ We have either $c = 0$, $b = a$ or $c = a, b = -a$. Thus $S(a)/\sim = \{S(a), -S(a)\}$. Proposition 3.1 yields that $\{S(a) \mid a \in G^*\}$ is an sdf.

Example 4.11. We note that for a left near-field $(F, +, \cdot)$ each element $a \in F^*$ induces an automorphism $\lambda_a : x \mapsto a \cdot x$ on $(F, +)$. Let $\Phi = \{\lambda_a \mid a \in F^*\}$. Then Φ is a group of fpf automorphisms of $(F, +)$, and Φ is isomorphic to $(F^*, \cdot)$.

With 1 denoting the identity of $(F, +, \cdot)$ we have $\lambda_1 = \mathbf{1}$. If $(F, +, \cdot)$ is not a field, then we do not have $\mathbf{1} - \lambda_a = \lambda_{1-a}$ in general. While $\mathbf{1} - \lambda_a$ for $a \neq 1$ is an automorphism of $(F, +)$, in general it is not true that $\mathbf{1} - \lambda_a \in \Phi$. We note that

$$\Phi \cap (\mathbf{1} - \Phi) = \{\lambda_a \mid a \in F^* \text{ such that } (1-a)x = x - ax \text{ for all } x \in F\}.$$

Let $(F, +, \cdot)$ be a Dickson near-field with Dickson pair (q, n). That is $(F, +, \cdot)$ is coupled to the field $\mathrm{GF}(q^n) = (F, +, *)$. Let $\Phi = \{\lambda_f \mid f \in F^*\}$. Then there exist $a, b \in F$ such that Φ is generated by $\alpha : x \mapsto a * x$ and $\beta : x \mapsto b * x^q$. That is, Φ, and hence $(F^*, \cdot)$ is metacyclic. Let $S^* \subseteq \Phi$ and $S = \mathbf{1} - S$. By Lemma 4.3 we have that $\langle S^* \rangle \subseteq \langle \alpha \rangle$, and in particular, $\langle S^* \rangle$ is cyclic. All mappings in S are of the form $\mu_f : x \mapsto f * x$ where $f \in \mathrm{GF}(q^n)$ and $*$ is the multiplication in the field $\mathrm{GF}(q^n)$.

Let $T = \{f \in F \mid \mu_f \in S\}$. Then $S(x) = T * x$ for all $x \in F$. Since T is central in the multiplicative group of $\mathrm{GF}(q^n)$, Corollary 3.5 yields that $\{T * x \mid x \in F^*\}$ is an sdf.

5. Conclusion and further work

This paper has presented an explanation of the creation of designs from planar near-rings as pioneered by Ferrero and Clay, using a generalization of the well known concept of difference families. A further analysis of work with segments was possible, both in its geometric view (the definition of segments by their endpoints) and the design view (determination of some of the resulting designs).

No clear understanding of the relation of circularity [BFK96, Ke92, KK96] to this structure has been seen. Future work may investigate this, as it seems to relate strongly to the motivating examples of planar near-rings from the complex plane, as does the segments construction.

References

[BFK96] K. Beidar, Y. Fong, and W.-F. Ke. On finite circular planar nearrings. *J. Algebra*, 185(3):688–709, 1996.

[BJL99] Thomas Beth, Dieter Jungnickel, and Hanfried Lenz. *Design theory. Vol. I.* Cambridge University Press, Cambridge, second edition, 1999.

[Bro01] Ron Brown. Frobenius groups and classical maximal orders. *Mem. Amer. Math. Soc.*, 151(717):viii+110, 2001.

[CD96] Charles J. Colbourn and Jeffrey H. Dinitz, editors. *The CRC handbook of combinatorial designs.* CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1996.

[Cla92] James R. Clay. *Nearrings.* The Clarendon Press Oxford University Press, New York, 1992. Geneses and applications.

[Ke92] W-F Ke. *Structures of circular planar nearrings.* PhD thesis, University of Arizona, 1992.

[KK96] Wen-Fong Ke and Hubert Kiechle. Combinatorial properties of ring generated circular planar nearrings. *J. Combin. Theory Ser. A*, 73(2):286–301, 1996.

[Sun01] Hsin-Min Sun. Segments in a planar nearring. *Discrete Math.*, 240(1-3):205–217, 2001.